International Journal of Computer Science Engineering
and Information Technology Research(IJCSEITR)
ISSN (P): 2249-6831; ISSN (E): 2249-7943
Vol. 8, Issue 3, Aug 2018, 9-16
© TJPRC Pvt. Ltd

TRANS STELLAR
•Journal Publications •Research Consultancy

SECURING ENCRYPTED SHARES USING STEGANOGRAPHY

NORA NAIK[1], PRATIK NAYAK[2], SHEHZEEN SHAIKH[3], EPHRAIM RODRIGUES[4] & YOGINI LAMGAONKAR[5]

[1]*Assistant Professor, Department of Computer Engineering, Agnel Institute of Technology & Design, Goa, India*

[2,3,4,5]*Student, Department of Computer Engineering, Agnel Institute of Technology & Design, Goa, India*

ABSTRACT

When it comes to security, the two major objectives are maintaining the secrecy and confidentiality of the data. Data can be secured in 2 ways, the first being completely changing the form of data into non-readable form. While the second being the hiding of the important data into some other random data. In this paper, we propose a scheme wherein we use the combination of both these techniques i.e changing the form of data first and then hiding it into some other data. The approach involves using the concept of sieving, dividing and shuffling for encrypting the data and LSB steganography technique to hide the data.

KEYWORDS: Sieve, Divide, Shuffle, Steganography, Encryption, Confidentiality & Secrecy

Received: Apr 20, 2018; **Accepted**: May 11, 2018; **Published**: Jul 06, 2018; **Paper Id.**: IJCSEITRAUG20182

Original Article

INTRODUCTION

The internet which introduced a new domain as to how data which is in the form of text, audio, video or an image can be transferred from one part of the world to another in real time. Sending of data should be in secure manner. However, along with these internet-based opportunities, it also increases the challenges such as maintaining the confidentiality and securing the data. Various research areas of cryptography can be used when it comes to protecting the data.

Cryptography is the process for generating security that helps prevent the intruders from obtaining the secret data and maintain the confidentiality of the data. It consists of encryption of data on the sender's side and its decryption on the receiver's side.

Considering the encryption domain, the traditional encryption techniques used algorithms such as RSA, DES etc. Which uses key approach. Using key for the encryption process key management is difficult. Another drawback of these techniques is that encryption keys are limited and it requires a heavy computation. This result into a new approach which includes splitting of an image at pixel level into n number of shares. Shares convey no information to the intruder at all, even if attacker attacks one of the shares, he will not able to obtain the original message. Receiver requires all the shares to regenerate the original information. And as an added level of security, steganography is applied to the shares.

RELATED WORK

Image Encryption (Using Keys)

This approach involves encrypting an image using an algorithm and a key. Digital signatures [2], vector quantization [4], chaos theory [3] etc. Are some of the proposed techniques for encrypting images. These techniques

involve certain limitations. It involves the use of keys and thus has all the limitations with regards to key management. Some times only a limited set of keys are available for encryption. Also, high computation is involved in computation process [5].

Image Splitting

This process involves splitting of an image into multiple shares at the pixel level. This ensures that the shares, individually convey no information about the image. And in order to regenerate the original image, the user needs to obtain all the shares. In 1979, Adi Shamir [6] was credited with introducing the idea of dividing the secret data into 2 random shares. Using this as the basis, in 1995, Naor and Shamir [7] proposed the concept of visual cryptography which involves secret sharing of an image by dividing it into multiple shares. The limitation of this approach is the loss of contrast and colors in the recovered image.

Visual Cryptography

One of the cryptographic techniques which allow visual information to be encrypted is termed as visual cryptography. Here, the decryption can be performed by humans without the aid of computers. This technique was initially introduced by Naor and Shamir in 1994. This method mainly involves a secret image to be shared amongst a qualified group who combine their shares to obtain the original image and a certain other group known as the forbidden group, who even after combining knowledge about their parts, do not get any information about the secret image. This approach gives a fast and easy decryption process.

PROPOSED TECHNIQUE

E-SPY (*Encrypted Shares Protecting You* A.K.A *Ephraim-Shehzeen-Pratik-Yogini*) Algorithm

The E-SPY technique involves creating multiple shares by splitting of an image. The original Secret image information is not revealed by the shares that are generated and all the shares are required in order to get the secret image. The technique involves 4 steps. Sieving, Dividing, Shuffling and Steganography. First step is sieving that is splitting of an image into its RGB color components. The second step is a division where in each of the color components is divided in an equal number of random parts. The third step is shuffling where in these divided parts of each color components are shuffled within itself. Finally, in order to generate the desired random shares, the shuffled components are combined. The fourth step involves applying steganography technique to these generated random shares. FIG 1 shows the steps involved in the process.

The most preferred models in order to represent colors are the additive and subtractive color models. RGB is an additive color model with three primary colors which is the RED, GREEN and BLUE the are mixed to get the colors that are required. Whereas CMYK is a subtractive color model in which the colors are represented by the degree of light reflected by the colored object. It is suitable to use an additive color model in this technique since it involves computation during the encryption and decryption stages and the results are to be viewed on the computer screen.

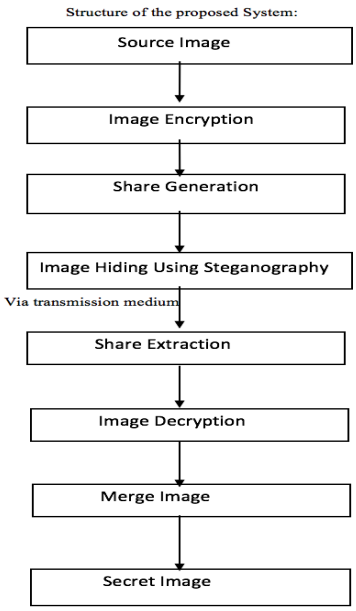

Figure 1: Structure of Proposed System

On a monitor screen consider an image to be a W*H 2-D matrix in which each entry represents a pixel value. Considering the image to be a 32 -bit colored image, each pixel is of 32 bits with each color component represented by 8 bits (8 bits each for RGB and final 8 bits for transparency). (Refer to figure 2)

	i=0	i=1	....	i=n-1
Red (8 bits)	R0	R1	....	R7
Green (8 bits)	G0	G1	....	G7
Blue (8 bits)	B0	B1	....	B7

Figure 2: Bit Representation

GENERAL WORKING OF E-SPY ALGORITHM

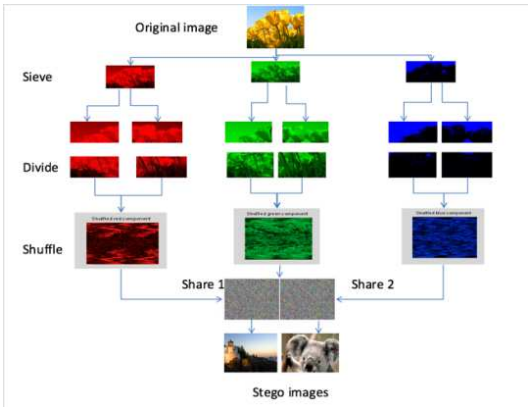

Figure 3: General Flow

Sieving

It is the splitting of the combined RGB components into individual R, G and B components (refer figure 4).. sieving uses the XOR operator in order to make the process computationally inexpensive.

Figure 4: Representation of Sieving Operation

Division

After splitting the original image into the R, G and B components, the next step is dividing the R, G and B components equally into z parts/ shares each.

- **R** ->(RA, RB, RC,----------, RZ)
- **G** ->(GA, GB, GC,----------, GZ)
- **B** ->(BA, BB, BC,----------, BZ)

While dividing it is ensured that each element in RA-Z, GA-Z and BA-Z is assigned random values, varying from 0- 255. The shares so generated should be such that (RA, RB, RC,---------- RZ) should regenerate R and similarly for G/B components. The zth share so generated is obtained by using the formula mentioned in the encryption algorithm which uses aggregate of each of the randomly generated shares of each color components and the values obtained of each color component after sieving the original image.(Refer figure 5).

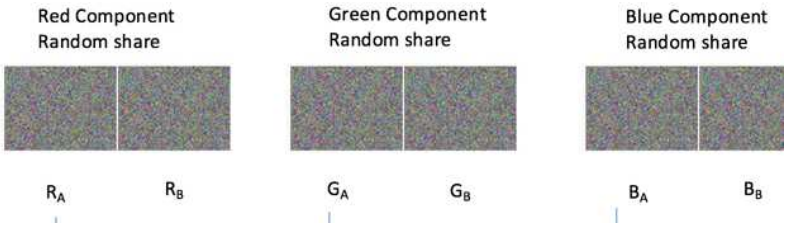

Figure5: Representation of Division Operation

Shuffling

In order to randomize the generated shares i.e. RA-Z, GA-Z and BA-Z, a shuffle operation is performed. A pixel-based odd-even shuffling is carried out in order to shuffle the elements within each of the individual divided shares.

- **RSA** -> (RA- shuffle, GA- shuffle and BA- shuffle)
- **RSB** -> (RB- shuffle, GB- shuffle and BB- shuffle)
- **RSZ** -> (RZ- shuffle, GZ- shuffle and BZ- shuffle)

Hence the random shares generated convey no information about the secret image individually, and all the random shares would be required to get back the original image. (refer Figure 6)

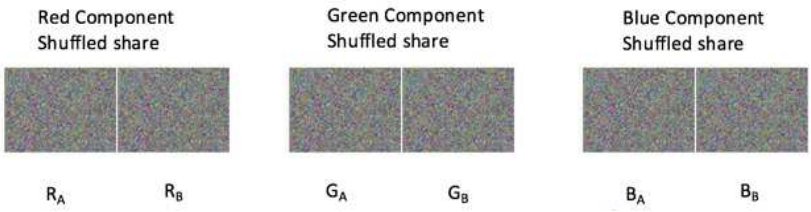

Figure 6: Shuffling Operation

Steganography

Once the final shares are obtained, as an increased level of security, steganography is applied on each share to make them more secure. As steganography hides the secret information on sight, the intruder is unable to detect the presence of any secret information.

For the proposed algorithm we make use of the LSB steganography technique which is embedding the bits of the secret image into each pixel of the cover image. (refer figure 7)

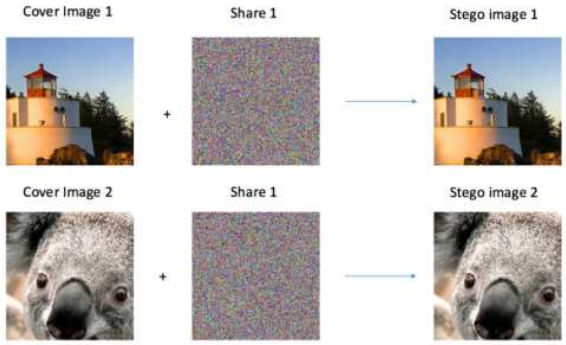

Figure 7: Representation of Steganography

E-SPY ALGORITHM

Step 1: Sieving

- Input Secret Image
- Sieve(Secret Image)
- Output (R, G, B components)

Step 2: Division

- **n** = total number of pixels (0 to n-1)
- **Ri** / Gi / Bi = individual values of the ith pixel in the R, G, B components
- **z =** total number of random shares
- **x** =number of bits representing each primary color
- max_val = 2x
- Repeat for R, G, B component

```
for i = 0 to (n-1)
{
for share k = A to (Z-1)
{
Rki = Random (0, max_val) ;
}
Aggr_Sumi= ΣRki ;
Mod_aggr_Sumi=Aggr_sumi % 256 ;
}
for i = 0 to (n-1)
{
Rzi=(max_val + Ri – (Aggr_Sumi % max_val))% max_val) ;
}
```

Step 3: Shuffle

```
Repeat for Rz, Gz and Bz(Last share) &Modded aggregate
For( i=0; i <Array.length() ; i++)
{
For( j=0; j < 8 ; i++)
{
a=DecToBin(j) ;
b=reverseBits(a) ;
c=BintoDec(b);
swap(Array[i][j]),Array[i][c]) ;
}
}
```

Step 4: Combine

- **Rz** = (Rz-shuffle XOR Gz-shuffle XOR Bz-shuffle)
- **Agg** = (Mod_Agg_Red-shuffle XOR Mod_Agg_Green –shuffle XOR Mod_Agg_Blue-shuffle)

Step 5: Steganography

Apply steganography on Rz & Agg Using 2 Cover images

EXPERIMENTAL RESULTS AND ANALYSIS

To improve the SDS algorithm[15], we came up with E-SPY algorithm to enhance the security and also improve its time and space utilization. We implemented this algorithm on java platform.

The scheme was run on a wide range of photographs including bright/dull images. We have demonstrated the result using a jpeg image titled as Lena.jpeg. It is 220 X 220 pixel image with an image depth of 24 bits (8-bits each for R/G/B components).

The various parameters as defined in the algorithm take the following values.

- **n** = (220*220) = 48400 (n varies from 0 to 48399)
- **z**= total number of random shares =2
- max_val = $2^x = 2^8 = 256$

The decryption process involves extraction of the shares from stego images obtained. And then sieving these shares to obtain the RA/GA/BA-shuffle.

Rz, Gz, Bz-shuffle which are then unshuffled to get

RA/GA/BA and Rz, Gz, Bz. And finally, obtain the original secret image using the decryption algorithm. The reconstructed image is obtained in totality whereas the recovered image quality in [13] is not exactly similar to the original secret image.

CONCLUSIONS

In this paper a new approach towards securing the data (image) is introduced wherein we apply Encryption and Steganography, hence enhancing the confidentiality and secrecy of the images and thus making it less vulnerable to the intruders. Key management is not an issue here since no keys are being used. The original (secret) image can be reconstructed in complete totality without any loss of data. Since, the final shares generated are limited to only 2, the space and the time required to process these shares is less. It has better security since it involves index based shuffling at a pixel level. By implementing steganography after encryption, the intruder is unable to detect the presence of the hidden image in some random image.

REFERENCES

1. *Xin Zhang and Weibin Chen, "A new chaotic algorithm for image encryption", International Conference on Audio, Language and Image Processing, 2008. (ICALIP 2008), pp 889-892.*
2. *Aloka Sinha and Kehar Singh, "A technique for image encryption using digital signature", Optics Communications(2003), 218(4-6), pp 229-234, online [http://eprint.iitd.ac.in/dspace/handle/2074/1161]*
3. *S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition 34 (2001), pp 1229-1245.*

4. *Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encryption algorithm for image cryptosystems", The Journal of Systems and Software 58 (2001), pp. 83-91.*
5. *S.Behnia,A.Akhshani,S.Ahadpour,H.Mahmodi,A. Akha-van, A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps,Physics Letters A 366(2007):391-396.*
6. *A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.*
7. *M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT' 94, Berlin, Germany, 1995, vol. 950, pp. 1–Springer-Verlag, LNCS.*
8. *Arpad Incze, "Pixel sieve method for secret sharing & visual cryptography" RoEduNet IEEE International Conference Proceeding Sibiu 24-26 June 2010, ISSN 2068-1038, p. 89-96*
9. *H.-C. Wu, C.-C. Chang, "Sharing Visual Multi-Secrets Using Circle Shares", Comput. Stand. Interfaces 134 (28),pp. 123–135, (2005).*
10. *Chin-Chen Chang, Jun-Chou Chuang, Pei-Yu Lin, "Sharing A Secret Two-Tone Image In Two Gray-Level Images", Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05), 2005.*
11. *Yadav, Rahul. "Message Security using Cryptography and LSB Algorithm of Steganography."*
12. *Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multiple-Image Encryption By Rotating Random Grids", Eighth International Conference on Intelligent Systems Design and Applications, pp. 252-256, 2008.*
13. *F. Liu1, C.K. Wu X.J. Lin, "Colour Visual Cryptography Schemes", IET Information Security, vol. 2, No. 4, pp 151-165, 2008.*
14. *Du-Shiau Tsai, Gwoboa Horng, Tzung-Her Chen, Yao-Te Huang, "A Novel Secret Image Sharing Scheme For True-Color Images With Size Constraint", Information Sciences 179 3247–3254 Elsevier, 2009.*
15. *C.C. Thien, J.C. Lin, "Secret image sharing", Computers & Graphics, Vol. 26, No. 5, 2002, pp. 765-770.*
16. *"A Keyless Approach to Image Encryption" Siddharth Malik, Anjali Sardana (2011).*